THE STUDY OF RISK MANAGEMENT DECISIONS DUE TO THE INVOLVEMENT OF THIRD PARTIES WITH INDIAN FINANCIAL INSTITUTION

Synopsis

Submitted in the partial fulfilment for the requirement of

Doctor of Philosophy

In

Management

Submitted by

Mr. JAYANT PRATAP SINGH

Under the supervision of

PROF. SUNITA KUMARI MALHOTRA

(Supervisor)

Department of Management

Faculty of Social Sciences, DEI

PROF. RAVI SHANKAR

(Co-Supervisor)

Department of Management

IIT, Delhi

Department of Management, Faculty of Social Sciences

Dayalbagh Educational Institute (Deemed to be University)

Dayalbagh, Agra-282005

2023

SECTION 1: INTRODUCTION

1. The Indian financial sector

India's economic success, which is heavily reliant on the financial sector, is not only a crucial source of global economic stability but also a source of enormous economic opportunity. The Indian financial industry has been profoundly affected by the vast developments in the Indian economy since liberalization in the early 1990s. The financial sector in India has been one of the fastest-growing in the country. The economy has seen a surge in private sector activity, including an influx of foreign banks, insurance firms, mutual funds, venture capital firms, and investment firms.

Since liberalization, the government and authorities have made a number of initiatives to confront the challenges of a complex financial architecture, ensuring that the Indian financial sector has taken on a new face, culminating in a strong, transparent, and resilient system.

India has a diverse financial sector that is rapidly expanding, both in terms of established financial services firms' robust growth and new entrants into the market. Commercial banks, insurance firms, non-banking financial companies, co-operatives, pension funds, mutual funds, and other smaller financial institutions make up the sector. New businesses, such as payment banks, have lately been allowed to be established by the banking regulator, expanding the types of entities that operate in the industry. However, India's financial sector is primarily a banking sector, with commercial banks accounting for more than 64% of the financial system's total assets. There have been a number of new instruments and items introduced. Existing industries have been made available to new private players. Existing players have upgraded their product offers and distribution networks as a result of the entry of new players. Financial intermediaries have also steadily adopted internationally accepted standards for revenue reporting, asset classification, provisioning, and capital adequacy. This has given the financial sector a huge boost in terms of development and modernization. The goal in the future would be to reach worldwide standards in this area in the shortest time possible.

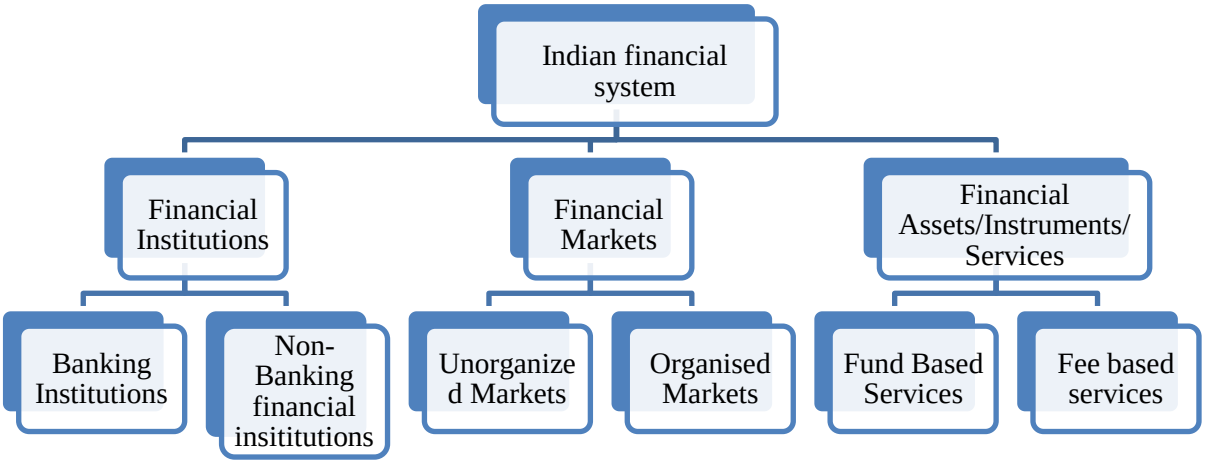

Figure 1: Indian financial system
(Source based: https://www.splessons.com/lesson/indian-financial-system-overview/)

2. Third-Party of the Indian financial system

For any organization, third party is any person, organization or firm which performs the business with them and the motive of doing that business is to generate more revenue and make their life easy. As per the collinsdictory website, the key definition of the third party is "a person who is involved by chance or only incidentally in a legal proceeding, agreement, or other transaction, especially one against whom a defendant claims indemnity" [2]

Hence if we talk about third parties we can consider two kinds of third parties for an organization one is a supplier and another is non-supplier.

Supplier: Suppliers are those third parties that provide/supply goods and/or services to the organization i.e. Fixed assets, offices, laptops and accounting tools, KYC solution and any other tools.

Non – Supplier: Non Supplier are those third parties that are exactly not suppliers but partners of the organization i.e. Branding partners, label partners and co-investors.

When we buy a card from HDFC we also got the stamp of VISA or MASTER over that that is one of the examples of Non supplier third party.

Scoping of the third party for the review

Currently, major markets are based on the services industry and the service industry has a direct impact on the consumers hence when it comes to the service industry, the suppliers that have maximum impact on companies hence my scope of research is suppliers only. We are scoping the review of this research to only the suppliers who deal in the services, i.e. those suppliers who provide either any service or any

tool-based solutions and there are furthermore service that any financial institute can get hence all those will be added in the scope.

2.1. Third-party risk

Risk is the measurable probability of the negative deviation of a target value from a reference value. (Heiko and Hinz 2004)

Third-party risk refers to the possible threat to an organization's employee and customer data, financial information, and operations posed by the organization's supply chain and other outside parties who offer products and/or services and have access to privileged systems. This is especially important since these outside parties frequently do not have the same security requirements and protection as the company, and as a result, they are exploited as a conduit into the business.[3]

Outsourcing operations to third-party contractors has been a common business approach since it helps companies to save money while also improving their operational efficiency. The importance of having vendor management practices in place grows as the involvement of third-party providers develops. Because vendors have access to important systems and consumer data, it's critical that your company keeps an eye on its cybersecurity risk to avoid any possible attacks.

When it comes to vendor management, using a risk-based strategy necessitates a thorough awareness of the many categories of vendor risk. Knowing this helps businesses to effectively assess third-party risk and classify providers according to the level of harm they offer

2.1.1. Type of third-party risk[4]

1. Cybersecurity risk
2. Compliance risk
3. Reputational risk
4. Financial risk
5. Operational risk
6. Strategic risk

Cybersecurity Risk

Cybersecurity risk is the probability of exposure or loss resulting from a cyber-attack or data breach on your organization. A better, more encompassing definition’s is the potential loss or harm related

to technical infrastructure, use of technology or reputation of an organization

Focus on compromised systems within vendor network settings while measuring performance. While data losses are not always the consequence of system breaches, they do give insight into how providers detect and mitigate assaults.

Compliance Risk

Compliance risk is the risk that arises from violations of laws, regulations, and internal processes that your organization must follow to conduct business. The laws that apply to each organization will vary by sector, however, there are some common regulations that span across industries such as GDPR(General Data Protection Regulation) and PCI DSS(Payment Card Industry Data Security Standard). Non-compliance with these regulations usually results in substantial fines so it is crucial that you make sure that your vendor’s cybersecurity compliance efforts align with regulatory requirements.

Reputational Risk

The public perception of your firm is the subject of reputational risk. Third-party vendors can damage your reputation in a number of different ways, including:

- Interactions that are not in accordance with the company's requirements.
- Customer data loss or exposure as a result of carelessness or a data breach.
- Infractions of laws and regulations

Financial Risk

Third-party financial risk emerges when contractors fail to fulfil your organization's fiscal performance criteria. Vendors face two types of financial risk: exorbitant expenditures and losing income.

Excessive expenditures, if not addressed, can stymie corporate growth and lead to excessive debt. To keep expenses under control, you should perform frequent audits to ensure that vendor expenditure is in accordance with the terms of your contract.

Managing lost income begins with determining which vendors have a direct influence on your organization's revenue-generating operations.

Operational risk

When vendor procedures are shut down, operational risk arises. Third-party operations are inextricably linked to organizational operations, thus when vendors fail to deliver on their promises, organizations frequently fail to carry out their daily operations. To reduce operational risk, your firm should develop a business continuity strategy so that you can continue to operate in the case of a vendor closure.

Strategic risk

Strategic risks develop when vendors make commercial decisions that will not coincide with the strategic objectives of your firm. The strategic risk may have an impact on compliance and reputational risk, and it is frequently a determining element in a company's total worth. Key performance indicators (KRIs) enable enterprises to successfully monitor strategic risk by providing significant information into vendor operations and procedures.

Third-party Risk Management (TPRM)

Third-party risk management is also called the supplier risk management process.

“Third-party risk management (TPRM) is a form of risk management that focuses on identifying and reducing risks relating to the use of third parties (sometimes referred to as vendors, suppliers, partners, contractors, or service providers).”[5]

While exact meanings differ, the word "third-party risk management" is frequently interchanged with other industry terminologies such as vendor risk management (VRM), vendor management, supplier risk management, and supply chain risk management. TPRM, on the other hand, is frequently conceived of as a broad discipline that incorporates all forms of third parties and risks.

The typical risk management process has 5 basic steps

1. **Risk identification**
2. **Risk assessment**
3. **Risk quantification**
4. **Risk mitigation and control**
5. **Risk monitoring**

It is suggested that when developing a third-party risk management programme, the process be divided into two stages[6]

1. Initial setup of the Third-Party Risk Management program
2. The ongoing monitoring of the Third-Party Risk Management program

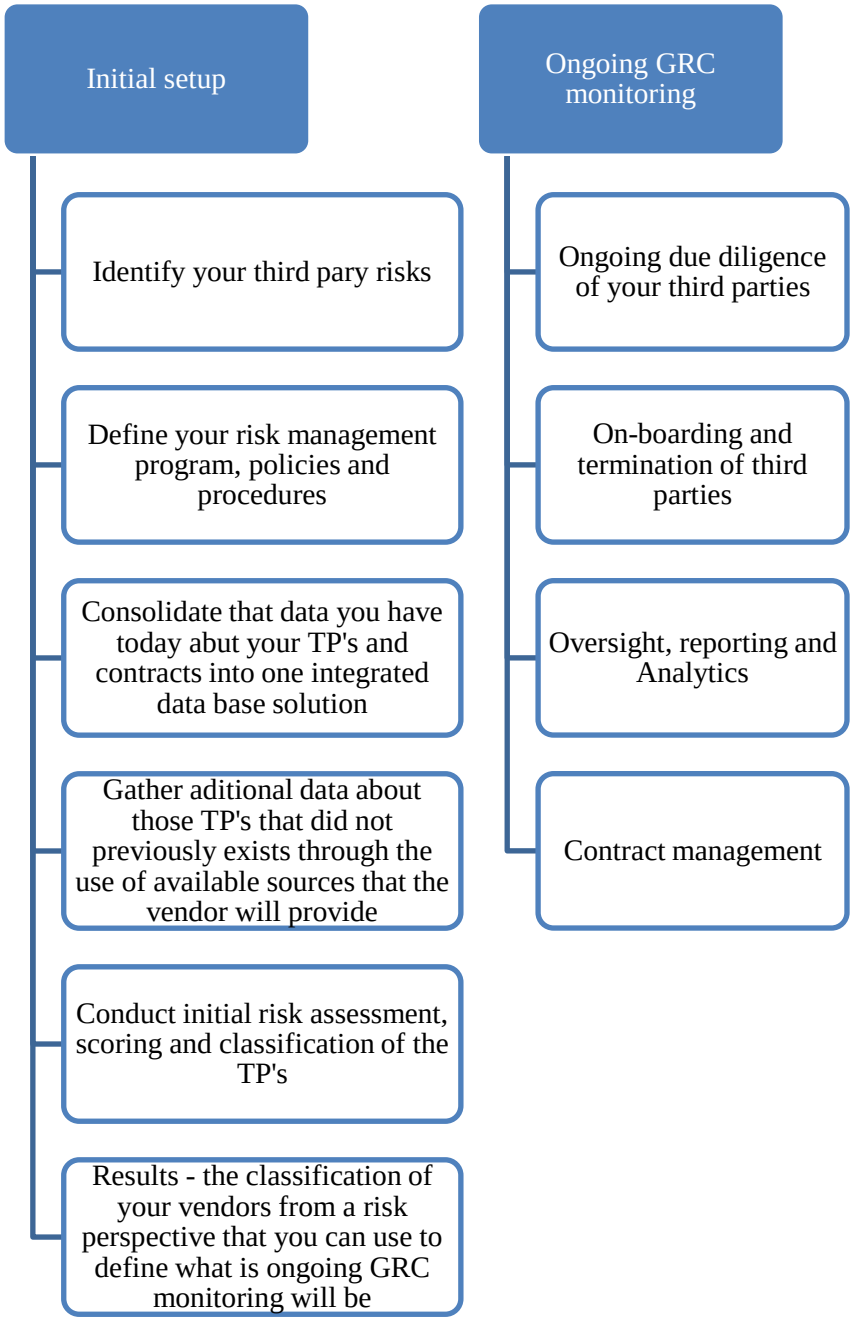
Initial setup
Identify your third pary risks
Define your risk management program, policies and procedures
Consolidate that data you have today abut your TP's and contracts into one integrated data base solution
Gather aditional data about those TP's that did not previously exists through the use of available sources that the vendor will provide
Conduct initial risk assessment, scoring and classification of the TP's
Results - the classification of your vendors from a risk perspective that you can use to define what is ongoing GRC monitoring will be
Ongoing GRC monitoring
Ongoing due diligence of your third parties
On-boarding and termination of third parties
Oversight, reporting and Analytics
Contract management

Figure 2. Framework for a Third party (TP) Risk Management Program
(Source based on : https://www.corporatecomplianceinsights.com/wpcontent/uploads/2017/11/Framework-for-a-Third-Party-Risk-Management-Program-2016-09-22-13.58.pdf)

Section 2: REVIEW OF LITERATURE

A literature review was conducted to gain a better understanding of the broad idea of third-party risk and its impact on organisations. A broad classification of the literature was performed by the researcher Table 1 at the end of this section contains a summary of the literature evaluated under the given classification.

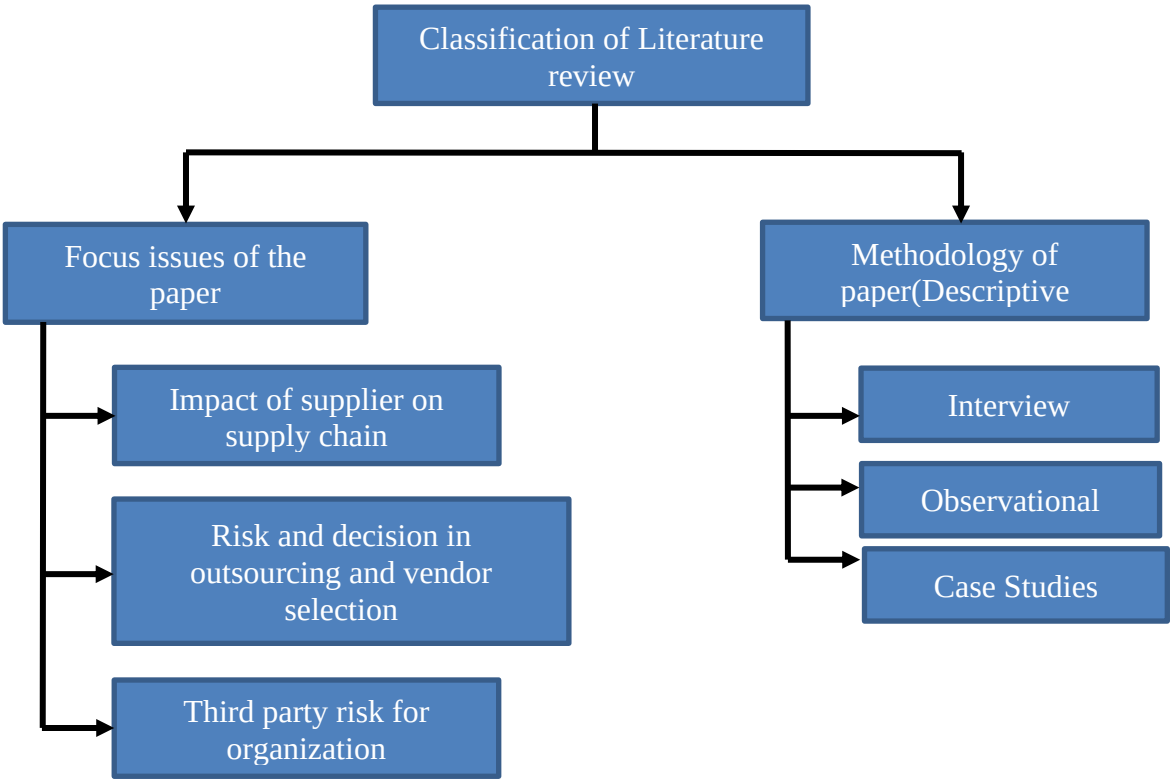

Figure 3: Approach for literature review
(Source: Self-constructed)

2.1. Paper content: Available literature can be broadly classified into three parts

2.1.1. Literature around the study of supply chain risk through Supplier risk

The first part emphasizes the supply chain risk as whenever a supplier is engaged it bring some external and internal risk to the organization and it will also bring some uncertainty to the supply chain.

Risk management has been incorporated into networks in only a few studies. Despite the fact that certain research has highlighted the unique characteristics of the network and These studies are about purchasing and outsourcing (Lonsdale, 1999), (Larry and Sue, 1998). There are other studies on the potential risks in the supply chain between small and large enterprises (Zanger, 1997), as well as the

challenges connected with common goals and insufficient information exchange in supply networks(Zanger, 1997), (Akkermans and Bogerd, 1999).

Since problems in networks can come from complicated chains that are difficult to identify, risk identification is an important aspect of the risk management process. The dynamics of relationship development add to the complexity. Companies in networks should communicate and share their risk perspectives since diverse perspectives aid in recognizing and comprehending common opportunities and threats in a more holistic manner. As a result, a greater understanding aids in making better decisions and reduces the risks faced by both a primary company and a network as a whole (Jukka, Iris, Urho, velli and Markku, 2004)

2.1.2. Literature around the study of risk and decisions in outsourcing and Vendor selection

Outsourcing, generally defined as the shifting of work done 'in-house' to another company, is thought of as a key strategy for improving cost and competitiveness (Kremic et al. 2006). Even cost is the first choice and it also gives us the flexibility in the rest of the operation as we need to put less emphasis on the outsourced processes. Effective supplier selection, innovative supplier development and meaningful supplier performance assessment have become key competencies needed for success (Kannan and Tan, 2002).

Due to supply chain interruptions, companies like Ericcson, Hershey, Apple, Wal-Mart, and a slew of others who rely on timely delivery of products and services from outsourcing to meet customer needs have suffered significant losses. Publicly traded companies that have had supply chain disruptions, for example, have documented negative stock market reactions to such news, with market capitalization drops as high as 10% (Knight and Pretty 1996, Hendricks and Singhal 2005). For example, , Ericsson reported a $400 million loss because it did not receive computer chip supply from a Philips plant on schedule (Latour 2001).

2.1.3. Literature around the study of third-party risk for complete Organization

Third-party risk is a relatively new concept for the organisation as it was not in the focus for the last few decades but we could find a few papers which are published the need for third-party risk assessment and method of assessing the supplier risk and method of managing the supplier risk. SRAM tool was developed that takes into account both operational capability indicators and financial indicators and

examines the issues of managing supplier risk and the accuracy of the estimations then it was applied to this model to the estimation of real-world supplier risk. (Kooyul, Youngdeok and Joongsan, 2011)

There is one important paper (Keskin, Caramancion, KM, Raza and Tatar, 2021) regarding cyber third-party risk management, Cyber third party risk is one of the major risks from various other risks of third party risk but it has more impact than any other third party risk hence it is considered to be a priority for risk managers. Paper represented the various methods that are in use in cyber third-party risk management. This paper also advises that approach to calculate the risk on the basis of scoring the vendor in risk so we can compare it with other suppliers.

The author is giving risk scores to all the risk factors that can affect the whole organisation hence below process is established as a model of risk assessment (Gary, Mary, Charlotte, Kevin and Kellie, 2010)

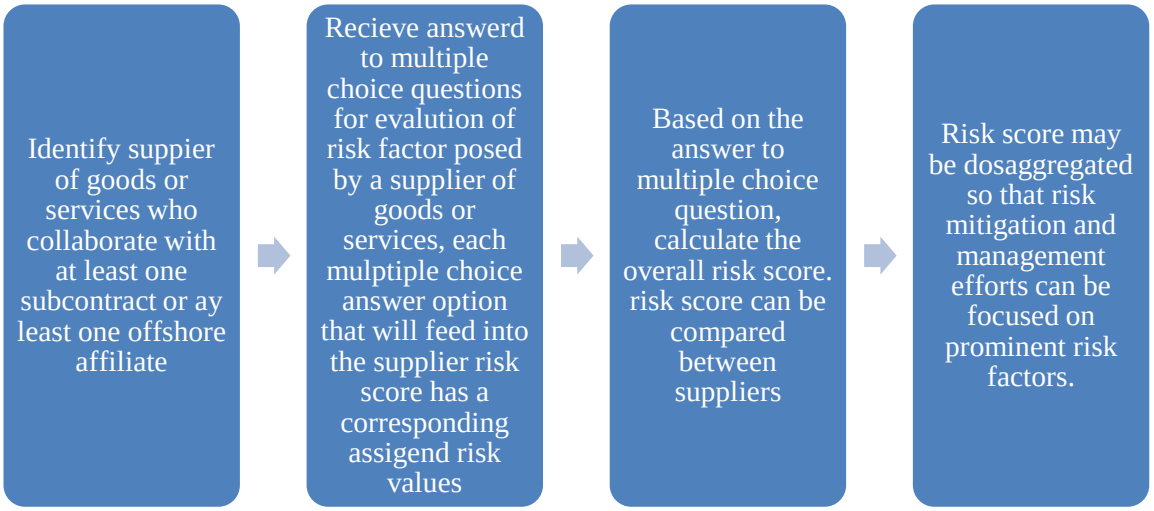
Identify suppier of goods or services who collaborate with at least one subcontract or ay least one offshore affiliate
Recieve answerd to multiple choice questions for evalution of risk factor posed by a supplier of goods or services, each mulptiple choice answer option that will feed into the supplier risk score has a corresponding assigend risk values
Based on the answer to multiple choice question, calculate the overall risk score. risk score can be compared between suppliers
Risk score may be dosaggregated so that risk mitigation and management efforts can be focused on prominent risk factors.

Figure 4 : Model of risk assessment

2.2. Methodology Approach

The literature review was divided into two categories at the second level, based on the research method adopted by the authors. This will give us an idea of the type of work that is done in a similar field.

2.2.1. Descriptive research

Descriptive research attempts to describe something like characteristics or functions of relevant groups, such as consumers, organizations and markets. It is also used to determine the degree to which variables are closely associated or to estimate the percentage of the population exhibiting certain characteristics. Based on the methodology adopted, descriptive research can be classified as below:

Interview and Survey based approach

In survey-based research, subjects complete a questionnaire natural setting to collect the data and analyst it over the course of time for population-representative results. Interview based research is common but it is one of the true pictures of results as it allows the responder to communicate and share his/her thoughts as it is because in different close-ended tools they cannot share their thoughts hence it is one of the ideal tools.

The researcher has taken a sample of 15 automotive casting suppliers to a major automotive company in the US and then after conducting survey they confirmed that their model is analysing risks in supply networks which can be used to facilitate outsourcing decisions. (Archie and Kevin 2010)

Research has taken a place with 2 organisational surveys and their cyber security risk rating is calculated and compared on the basis of normalisation factor (Keskin, Caramancion, KM, Raza and Tatar, 2021) (Vikas and Rakesh, 2015)

They have received a total of 114 questionnaires, of which 104 were complete (and thus usable). This sample size allowed them to perform a factor analysis, as the minimum sample size required to perform satisfactorily a factor analysis is 50 (Arrindell and Ende 1985). The respondents' profiles were diverse, ranging from third party, end-user, executive, SCM manager and hence it was resulted that there are six main risk factors that Indian companies are facing. These are cultural, operational, infrastructure, economic, forecasting and supplier risk. (Helen, Mohit, Kulwant and Janat, 2015)

Case study based approach

The case study approach is a way in which an individual component, such as an institution or a single occurrence in a person's or a group's life, is examined in connection to other members of the group. A life or case history is a pretty comprehensive examination of a person/group/organization (as to what they do and have done, what they think he does and has done, and what they expect to do and say he ought to do) or group. In a nutshell, the case study approach is a type of qualitative analysis in which an individual, a scenario, or an institution is observed carefully and thoroughly, and attempts are made to Analise each and every detail.

Below are a few researched that have been published on the basis of the case study.

(Jennifer, Kevin and Danny, 2008), (George, 2003), (Keskin, Caramancion, KM, Raza and Tatar, 202),

(Chris Lonsdale, 1999), (Larry and Sue, 1998), (Jukka, Iris, Urho, velli and Markku, 2004), (E Caruso, M Dicorato, A Minoia and M Trovato, 2006) (Merve and Seniye, 2018)(Gary, Mary, Charlotte, Kevin and Kellie, 2010)(Shashank and Thomas, 2009)

Observational based

A correlational approach to study is the observational approach. Nonexperimental research is defined as a study in which the researcher does not interfere or employ experimental control (e.g., manipulation, elimination, inclusion, group or condition assignment). When researchers want to measure the degree of association (i.e., relationship) between variables or forecast a specific outcome (criterion) depending on the predictor variable, they employ this method (s). Statistical techniques are the sole sort of control that can be employed in nonexperimental research and the observational approach. Some researchers and authors refer to the actual analysis as the research design because statistical techniques are the only kind of control that can be applied to the observational methodology.

(Gewald, Heiko , Hinz and Daniel 2004), (Tursoy and Turgut, 2018)

2.3 Case Studies/Survey published by private industries

There are various case studies and survey published by the private sector and student which talks about either third-party risk or organization is impacted due to third parties. There is a case study about Domino's data leak, the total size of the leak was 13TB of the employee files and 18 crore orders details which include the name of the person who orders it, phone number, address and address for the orders and complete order details. Then hackers demand the ransom of 50 BTC (21.3 Crores) and after that, there was no response from Domino's so the hacker made the whole data public by putting it on a public link. After investigation, it was noted that the reason for this leak is a compromise on the Amazon web services key which was a third party for Dominos.

Table 1: Summary of literature review

			Focus Issues				Context		Methodology		
Title Author Year	Category	Literature review	Supply chain	Third party risk	Outsourcing decision /Vendor section	Industry Specific	Indian	Foreign	Qualitative Survey/ interview based	Qualitative Case Study	Qualitative Observational
Jennifer V. Blackhurst, Kevin P. Scheibe, Danny J. Johnson, (2008),"Supplier risk assessment and monitoring for the automotive industry", International Journal of Physical Distribution & Logistics Management, Vol. 38 Iss: 2 pp. 143 - 165	International Journal	Yes				Automotive industry		Yes		Yes	
Gewald, Heiko and Hinz, Daniel, "A Framework for Classifying the Operational Risks of Outsourcing - Integrating Risks from Systems, Processes, People and External Events within the Banking Industry" (2004). PACIS 2004 Proceedings. 84.	International Journal	Yes			Yes	Banking industry		Yes			Yes

George A. Zsidisin, 2003 "A grounded definition of supply risk" Journal of Purchasing & Supply Management 9 (2003) 217–224	International Journal	Yes	Yes			Purchasing Industry		Yes		Yes	
Kooyul Jung, Youngdeok Lim and Joongsan Oh (2011), "A Model for Measuring Supplier Risk: Do Operational Capability Indicators Enhance the Prediction Accuracy of Supplier Risk?" British Journal of Management, Vol. 22, 609–627 (2011) DOI: 10.1111/j.1467-8551.2010.00697.x	British Journal	Yes		Supplier risk				Yes	Yes		
Archie Lockamy III & Kevin McCormack (2010) Analysing risks in supply networks to facilitate outsourcing decisions, International Journal of Production Research, 48:2, 593-611,DOI: 10.1080/00207540903175152	International Journal	Yes			Yes	Automotive industry		Yes	Yes		

Keskin, O.F. Caramancion, K.M. Tatar, Raza, O.; Tatar, U. Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports. Electronics 2021, 10, 1168 .https://doi.org/10.3390/electronics10101168	International Journal	Yes		Yes		Educational Institute		Yes	Yes	Yes	
Chris Lonsdale, (1999),"Effectively managing vertical supply relationships: a risk management model for outsourcing", Supply Chain Management: An International Journal, Vol. 4 Iss 4 pp. 176 - 183	International Journal	Yes			Yes	HP		Yes		Yes	
Desheng Dash Wu & David Olson (2010): Enterprise risk management: a DEA VaR approach in vendor selection, International Journal of Production Research, 48:16, 4919-4932	International Journal	Yes			Yes			Yes			
Larry R. Smeltzer and Sue P. Siferd(1998) "Proactive Supply Management:The Management of Risk", International Journal of Purchasing and Materials Managemen	International Journal	Yes	Yes			Purchasing Industry		Yes		Yes	

Aseem Kinra, Dmitry Ivanov, Ajay Das & Alexandre Dolgui (2019): Ripple effect quantification by supplier risk exposure assessment, International Journal of Production Research, DOI: 10.1080/00207543.2019.1675919	International Journal	Yes	Yes			Manufacturing industry		Yes			
Tursoy, Turgut (2018), "Risk management process in banking industry" MPRA Paper No. 86427, posted 02 May 2018 14:20 UTC	Paper	Yes				Banking Industry		Yes			Yes
Jukka Hallikasa, Iris Karvonenb, Urho Pulkkinen, Veli-Matti Virolainen, Markku Tuominen (2004), Risk management processes in supplier networks, Int. J. Production Economics 90 (2004) 47–5	International Journal	Yes	Yes			Manufacturing industry		Yes		Yes	
E . Caruso, M. Dicorato, A. Minoia and M. Trovato,(2006),"Supplier risk analysis in the day-ahead electricity market" IEE Proc.-Gener. Transm. Distrib., Vol. 153, No. 3	International Journal	Yes				Electricity		Yes		Yes	

Merve Er Kara and Seniye Ümit Oktay Fırat (2018), "Supplier Risk Assessment Based on Best-Worst Method and K-Means Clustering: A Case Study" Multidisciplinary Digital Publishing Institute,	International Journal	Yes	Yes			Undefined		Yes		Yes	
Vikas Thakur Ramesh Anbanandam , (2015),"Supplier Selection Using Grey Theory: A Case Study from Indian Banking Industry", Journal of Enterprise Information Management, Vol. 28 Iss 6 pp. -	International Journal	Yes	Yes						Yes		
Helen Rogers, Mohit Srivastava, Kulwant S Pawar & Janat Shah (2015): Supply chain risk management in India – practical insights, International Journal of Logistics Research and Applications: A Leading Journal of Supply Chain Management, DOI: 10.1080/13675567.2015.1075476	International Journal	Yes	Yes				Yes		Yes		
Desheng Wu, David L. Olson, (2008) ,"Supply chain risk, simulation, and vendor selection" Int. J.	International Journal	Yes	Yes					Yes			

Production Economics 114 (2008) 646– 655											
Shashank Rao, Thomas J. Goldsby, (2009) "Supply chain risks: a review and typology", The International Journal of Logistics Management, Vol. 20 Issue: 1, pp.97-123, https://doi.org/10.1108/09574090910954864	International Journal	Yes	Yes							Yes	
Robert Stroud (2014) Vendor Risk Management Using COBIT 5, EDPACS: The EDP Audit, Control, and Security Newsletter, 50:1, 11-17, DOI: 10.1080/07366981.2014.922837	International Journal	Yes	Supply chain					Yes			
Vijay R. Kannan; Keah Choon Tan, 2002, "Supplier Selection and Assessment: Their Impact on Business Performance" Journal of Supply Chain Management DOI: 10.1111/j.1745-493x.2002.tb00139.x	International Journal	Yes			Yes	Manufacturing industry		Yes	Yes		

VahidNourbakhsh, Abbas Ahmadi and MasoudMahootchi (2013) "Considering supply risk for supplier selection using an integrated framework of data envelopment analysis and neural networks" International Journal of Industrial Engineering Computations 4 (2013)273–284	International Journal	Yes	Yes					Yes			
Gary Francis Page, Mary Frances Edwards, Charlotte, Kevin Michael Woerner, Charlotte,Kellie Lyn McCorvey,(2010)"SUPPLIER RISK EVALUATION", Patent Application Publication, US 2010/0198630 A1	Patent			Yes		Financial		Yes		Yes	

3. Section 3

3.1. Research gap

1. There are not much research performed addressing the third-party risk aspect of research, the following are some gaps.

a. **Limited to international markets (Most of the researches are for the US**): out of the available literature we have noted that all the researches are pertain to the international markets and none of them is pertaining to third-party risk and the Indian fiancé sector.

b. **Researches are limited to impact of third party/supplier risk on supply chain:** it is also being noticed that researches are talking about the impact of third party risk on the supply chain only but when we talk about the whole organisation, it has various arms which are also important apart from the supply chain management hence these arms should also be considered so we have stated that it is also a limitation.

c. **Most of the available literature is for the manufacturing industry:** when we talk about the industries covered with the research then most of this research are only talk about the manufacturing industries or only those company that manufacture a tangible product.

2. When we analyze these gaps, we could comment on the gap fillers hence below are a few identified gap-fillers:

a. **Indian Market:** As most of the research has been done in the international market, we can consider the Indian market for the research which will definitely add value to the literature.

b. **Impact of third-party risk on other pillars of business**: as mentioned above a few research talks about the third-party risk on the end to end organization hence we can fill it by performing research.

c. Service industry: Service industry is one of key thing missing from our literature we can think about the organization's risk that engaged in the service industry.

3.2. Motivation of current research

After going through the literature review it is noticed that the majority of the literature is available for risk in the supply chain management or it can also be addressed as this literature is about measuring the impact of suppliers in the supply chain which leads the focus of various research on supply chain

only while case studies show that we have major risk on the enterprise level from the supplier which needs to be assessed, calculated, monitored, controlled and mitigated.

"Indian companies have set the most aggressive cost reduction targets in the APAC region, with 44 per cent of companies looking at cost reduction targets of up to 20 per cent. However, 63 per cent of companies have reported failure in meeting cost reduction targets in the past," said Gaurav Gupta, Partner, Deloitte Touche Tohmatsu India LLP.[7] Most of the industries are either outsource or bring new technologies for cost reduction. (K Ketler; J Walstrom, 1993) which means more third parties will be engaged.

As per a report, India ranked third in the world in terms of the number of data breaches, with a total of 86.63 million Indian users breached till November 2021. he reports from cybersecurity company Surfshark used its own breach detection mechanism. India showed a 351.6 per cent increase in affected accounts compared to last year. In 2020, around 19.18 million Indian users' data was breached. "In general, this year was slightly worse than the last in terms of data breach cases," the report said.[8]

These breaches lead any organisation to reputational loss, financial loss and regulatory fines hence it can be said that the whole organisation will be impacted.

(Jennifer, Kevin and Danny, 2008) Developed the supplier risk assessment framework for measuring, tracking, and analysing supplier and part-specific risk for the Automotive industry. While we need to see enterprise as a whole.

Biggest data breaches in 2021

S. No.	Data Breach	Size
1	Dominos India	18cr
2	Mobikwik	10cr
3	Facebook	60lakh
4	Air India	45lakh
5	Upstox	25lakh

Figure 5: Source based - https://www.91mobiles.com/hub/5-major-data-breaches-india-2021/

The above picture shows the total number of a data breaches in 2021 and out of these 5 breaches reason for 3 breaches is third parties' solutions hence we can see it is a must that we need to put more emphasis on third party risk solutions.

3.3. Research Question:

Based on the research gaps identified, it is proposed to address the following questions:

- What are the different risks that are triggered from third-party relationships in an organization if we consider an organization as a whole?
- To what extent does third party risks impact the organization in the Indian financial sector?
- Do we really need a third-party risk management program in the Indian financial sector?
- How to choose which third-party risk management program is suitable for the organization?

3.4. Research Objectives:

The proposed study will address the following major objectives:

- To find out the various risk associated with third-party relationships in the Indian financial institutions.
- To study the need for third-party risk management programs in the Indian financial institution
- To assess the impact of third-party risk management program decisions on the selected risks categories.
- To recommend the way forward to third party risk managers in order to choose the best third-party risk management solution for their organization in order to manage the end-to-end risk.

3.5. Conceptual Framework and Hypothesis Development

In this section, a conceptual framework is proposed depicting the impact of various risks (that arise from the third-party relation) on the entire organisation. While going through case studies and various literature available over the internet.

The conceptual framework(Figure 6) explains the approach followed in this research. we shall consider all the variable risk pillar (Information security, Compliance, Financial risk, business continuity risk, government relation and political exposure) of any financial organisation which plays a vital role in an organisation's success or failure. Third party risk management decisions and we are central to this

framework, shall try to establish a connection between the third party risk management decision and variable risk pillars that either third party risk management decision impact these variable or not and then on the right-hand side you can see we have organisation goodwill and reputation so we are trying to show how third party risk management decision is directly and indirectly(through variables) impact the organisational goodwill and reputation. The third-party risk management decision are majorly play the role of the risk mitigation component and it

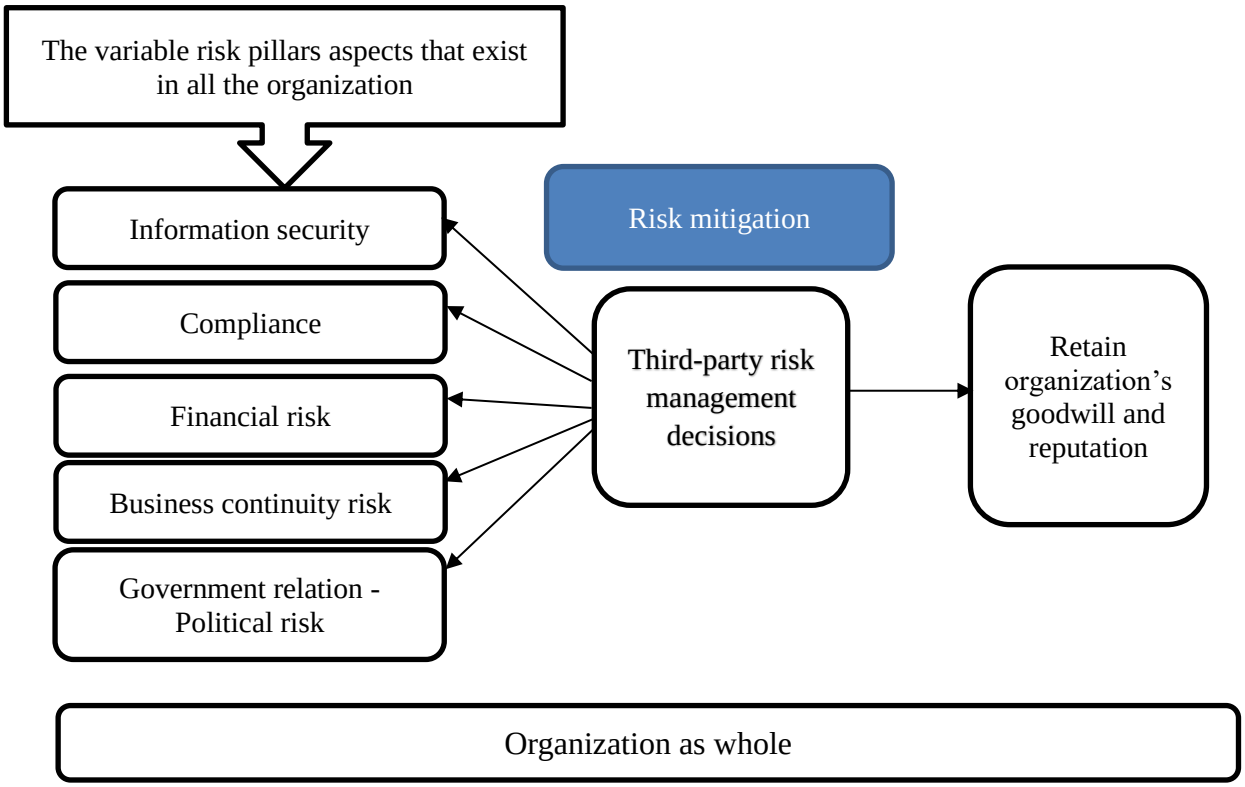

Figure 6: Research framework
(Source: Self-constructed)

PROPOSED HYPOTHESES AS PER THE CONCEPTUAL FRAMEWORK:

- **Impact of third-party risk management decisions on an organization's information security system.**

Information security, abbreviated as infosec, refers to a collection of procedures for protecting data from unauthorized access or alteration while it is being stored as well as when it is being transmitted from one system or physical location to another. It's also referred to as data security on occasion. As knowledge has grown in importance as one of the most valuable assets in the twenty-first century,

attempts to keep information secure have grown in importance as well. While it is that important part of an organisation hence, we need to see how it will be impacted by the third-party risk management decision.

Ho1: There is no impact of third-party risk management decisions on an organization’s information security system.

Ha1: There is an impact of third-party risk management decisions on an organization’s information security system.

- **Impact of third-party risk management decisions on the Compliance risk**

An organization's potential exposure to legal fines, financial forfeiture, and material loss as a result of failing to behave in line with industry laws and regulations, internal policies, or recommended best practices is known as compliance risk. Integrity risk is another name for compliance risk.

Compliance risk affects all types and sizes of businesses, whether they are public or private, for-profit or charity, state or federal. Failure to comply with applicable rules and regulations can harm an organization's revenue, as well as its reputation, commercial opportunities, and valuation.

while compliance risk also a backbone for system of any organisation so we need to check the impact of third-party risk management decision on this.

Ho2: There is no impact of third-party risk management decisions on compliance risk.

Ha2: There is an impact of third-party risk management decisions on compliance risk.

- **Impact of third-party risk management decisions on the financial pillar.**

Financial pillar is one of the key strengths of any organization as it controls the flow of money in the organization and there are many times when this flow is controlled by any third party which leads to any error or fraud hence it is one of the factors where we need to see the impact.

Ho3: There is no Impact of third-party risk management decisions on the financial pillar.

Ha3: There is an Impact of third-party risk management decisions on the financial pillar.

- **Impact of third-party risk management decisions on business continuity.**

Business continuity refers to the planning and preparation done ahead of time to ensure that an organization's critical business functions can continue to operate in the event of an emergency. Natural catastrophes, business crises, pandemics, workplace violence, or any other event that disrupts your

business operations are examples of events. It's crucial to remember that you should plan and prepare not just for incidents that will fully shut down operations, but also for those that may have a negative influence on services or functions.

Ho4: There is no Impact of third-party risk management decisions on business continuity.

Ha4: There is an Impact of third-party risk management decisions on business continuity.

- **Impact of third-party risk management decisions on government/ political issues.**

Business organizations can be influenced by the political climate in a variety of ways. It could introduce a risk factor and result in a significant loss. You should be aware that political forces have the ability to influence outcomes. It can also have an impact on government policies at all levels, from local to federal. Companies should be prepared to deal with the consequences of politics on a local and worldwide level.

Ho5: There is no Impact of third-party risk management decisions on government/ political issues.

Ha5: There is an Impact of third-party risk management decisions government/ political issues.

- **Comparison of the impact of third-party risk on selected risk pillars.**

Ho5: There is no Impact of third-party risk management decisions on the Information security pillar than the other risk pillars.

Ha5: There is a significant Impact of third-party risk management decisions on the Information security pillar than the other risk pillar.

Section 4: METHODOLOGY TO BE USED IN THE PROPOSED RESEARCH

4.1 Scope of Study

Area of the survey: India

Population: Total number of professionals working in Vendor/supplier risk department in the world

Target Population: Total number of Indian professionals working in the Vendor/supplier risk department in Indian financial institutions**.**

5.2 Sampling Plan

5.2.1 Sample Size Calculation

This research design requires a huge sample size for the purpose of representation. For the purpose of this study, the sample size determination formula for infinite population (‘unknown population’) used as

$$n = \frac{Z^2 * p(1-p)}{M^2}$$

The above given sample size formula for infinite population is used to arrive at a representative number of respondents when population estimate is known (Godden, 2004):

Where: n = Sample Size for infinite population

1. The standard deviation is .5.
2. The margin of error is 5%
3. The confidence level is 95 %

Sample size = 385

For Third-party risk management experts: Structured personal interview of 30 managers would be conducted.

5.3 Sampling Technique

The sampling technique will be a purposive sampling technique. Purposive sampling is a sampling method based on criteria that are related to the research objectives. The respondents would be the common employee who works in the stream of third-party risk management.

5.4 Data Collection Instruments

5.4.1 Primary Data Tools

The tools used for the purpose of primary data collection would be questionnaires, personal interviews and focused group discussion (both structured and unstructured).

- Questionnaires will be used for the survey of employees.
- Structured Personal Interviews will be conducted for third party risk management experts to understand the impact of third-party risk management decisions on the organisation as a whole.

5.4.2 Secondary data

Data will be collected through various magazines, journals, publications of business research agencies, the organisation's annual financial reports, surveys and reports published by private organisations.

5.5 Statistical Techniques for Data Analysis

Relevant analytical tools like descriptive statistics, z-test, ANOVA and Regression would be used on the collected data and further reviews will be done on the basis of interview data collected by the researcher.

Section 5: CHAPTERIZATION

The proposed study will contain the following chapters:

- Chapter 1: Introduction
- Chapter 2 – Review of Literature and Case Studies
- Chapter 3- Conceptual Framework
- Chapter 4 – Research Design and Methodology
- Chapter 5– Data Collection and Analysis
- Chapter 6– Analysis using structured equation modelling.
- Chapter 6– Results and Interpretations
- Chapter 7 –Managerial Implications, Conclusion and Direction for Future Research
- Bibliography and References
- Appendix

Reference

Papers:

1. Jennifer V. Blackhurst, Kevin P. Scheibe, Danny J. Johnson, (2008),"Supplier risk assessment and monitoring for the automotive industry", *International Journal of Physical Distribution & Logistics Management, Vol. 38 Iss: 2 pp. 143 - 165*

2. Gewald, Heiko and Hinz, Daniel, "A Framework for Classifying the Operational Risks of Outsourcing - Integrating Risks from Systems, Processes, People and External Events within the Banking Industry" (2004). *PACIS 2004 Proceedings. 84.*

3. George A. Zsidisin, 2003 "A grounded definition of supply risk" *Journal of Purchasing & Supply Management 9 (2003) 217–224.*

4. Kooyul Jung, Youngdeok Lim and Joongsan Oh (2011), "A Model for Measuring Supplier Risk: Do Operational Capability Indicators Enhance the Prediction Accuracy of Supplier Risk?" *British*

Journal of Management, Vol. 22, 609–627 (2011) DOI: 10.1111/j.1467-8551.2010. 00697.x

5. Archie Lockamy III & Kevin McCormack (2010) Analysing risks in supply networks to facilitate outsourcing decisions, *International Journal of Production Research, 48:2, 593-611, DOI: 10.1080/00207540903175152*

6. Amril Syalim, Yoshiaki Hori and Kouichi Sakurai (2009), "Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide" *International Conference on Availability, Reliability and Security*

7. Vahid Nourbakhsh, Abbas Ahmadi and Masoud Mahootchi (2013) "Considering supply risk for supplier selection using an integrated framework of data envelopment analysis and neural networks" *International Journal of Industrial Engineering Computations 4 (2013)273–284*

8. Keskin, O.F. Caramancion, K.M. Tatar, Raza, O.; Tatar, U. Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports. *Electronics 2021, 10, 1168 .https://doi.org/10.3390/electronics10101168*

9. Chris Lonsdale, (1999),"Effectively managing vertical supply relationships: a risk management model for outsourcing", *Supply Chain Management: An International Journal, Vol. 4 Iss 4 pp. 176 - 183*

10. Desheng Dash Wu & David Olson (2010): Enterprise risk management: a DEA VaR approach in vendor selection, *International Journal of Production Research, 48:16, 4919-4932*

11. JONATHAN HUGHES (2007), "Justice and Third Party Risk: The Ethics of Xenotransplantation" *Journal of Applied Philosophy, Vol. 24, No. 2, 2007*

12. Aineth Torres-Ruiz, A. Ravi Ravindran, Multiple Criteria Framework for the Sustainability Risk Assessment of a Supplier Portfolio, Journal of Cleaner Production (2017),doi: 10.1016/j.jclepro.2017.10.304

13. "Larry R. Smeltzer and Sue P. Siferd(1998) ""Proactive Supply Management: The Management of Risk"", *International Journal of Purchasing and Materials Management"*

14. Aseem Kinra, Dmitry Ivanov, Ajay Das & Alexandre Dolgui (2019): Ripple effect quantification by supplier risk exposure assessment, *International Journal of Production Research, DOI: 10.1080/00207543.2019.1675919*

15. Tursoy, Turgut (2018), ""Risk management process in banking industry"" *MPRA Paper No. 86427, posted 02 May 2018 14:20 UTC"*

16. Jukka Hallikasa, Iris Karvonenb, Urho Pulkkinen, Veli-Matti Virolainen, Markku Tuominen (2004), Risk management processes in supplier networks, *Int. J. Production Economics 90 (2004) 47–5*

17. E . Caruso, M. Dicorato, A. Minoia and M. Trovato,(2006),"Supplier risk analysis in the day-ahead electricity market" *IEE Proc.-Gener. Transm. Distrib., Vol. 153, No. 3*

18. Merve Er Kara and Seniye Ümit Oktay Fırat (2018), "Supplier Risk Assessment Based on Best-Worst Method and K-Means Clustering: A Case Study" *Multidisciplinary Digital Publishing Institute,*

19. Gary Francis Page, Mary Frances Edwards, Charlotte, Kevin Michael Woerner, Charlotte,Kellie Lyn McCorvey,(2010)"SUPPLIER RISK EVALUATION", *Patent Application Publication, US 2010/0198630 A1*

20. Vikas Thakur Ramesh Anbanandam , (2015),"Supplier Selection Using Grey Theory: A Case Study from Indian Banking Industry", *Journal of Enterprise Information Management, Vol. 28 Iss 6 pp.*

21. Helen Rogers, Mohit Srivastava, Kulwant S Pawar & Janat Shah (2015): Supply chain risk management in India – practical insights, *International Journal of Logistics Research and Applications: A Leading Journal of Supply Chain Management, DOI: 10.1080/13675567.2015.1075476*

22. Desheng Wu, David L. Olson, (2008) ,"Supply chain risk, simulation, and vendor selection" I*nt. J. Production Economics 114 (2008) 646– 655*

23. Shashank Rao, Thomas J. Goldsby, (2009) ""Supply chain risks: a review and typology"", The *International Journal of Logistics Management, Vol. 20 Issue: 1, pp.97-123, https://doi.org/10.1108/09574090910954864"*

24. B.J.M. Ale and M. Piers, (2000) , "The assessment and management of third party risk around a major airport"*Journal of Hazardous Materials 71 2000. 1–16*

25. Chengpeng Jiang, Henk A.P. Blom and Alexei Sharpanskykh (2020) "Third Party Risk Indicators

and Their Use in Safety Regulations for UAS Operations" *UNIVERSITY OF GLASGOW on June 28, 2020 | http://arc.aiaa.org | DOI: 10.2514/6.2020-2901*

26. Robert Stroud (2014) Vendor Risk Management Using COBIT 5, EDPACS: *The EDP Audit, Control, and Security Newsletter, 50:1, 11-17, DOI: 10.1080/07366981.2014.922837*

27. Lonsdale, C., 1999. Effective managing vertical supply relationships: A risk management modelfor outsourcing. *Supply Chain Management: An international Journal 4 (4), 176–183.*

28. Zanger, C., 1997. Opportunities and risks of network arrangements among small and large firms within supply chain. *Paper presented in the Sixth International Annual IPSERA Conference, Naples*

29. Akkermans, H., Bogerd, P., Vos, B., 1999. Virtuous and vicious cycles on the road towards international supply chain management. *International journaled Operations and Production Management 19 (5/6), 566–581.*

30. Vijay R. Kannan; Keah Choon Tan, 2002, ""Supplier Selection and Assessment: Their Impact on Business Performance"" *Journal of Supply Chain Management DOI: 10.1111/j.1745-493x.2002.tb00139.x"*

31. Kevin B. Hendricks; Vinod R. Singhal, (2005), "An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-Run Stock Price Performance and Equity Risk of the Firm" *Production and Operations Managementvolume 14, issue 1 (2005) DOI: 10.1111/j.1937-5956.2005.tb00008.*

Website for details and Definition

1. https://www.ibef.org/industry/financial-services-presentation
2. https://www.collinsdictionary.com/dictionary/english/third-party#:~:text=A%20third%20party%20is%20someone,it%20in%20a%20minor%20role.
3. https://awakesecurity.com/glossary/third-party-risk/
4. https://securityscorecard.com/blog/six-types-of-vendor-risk-that-are-important-to-monitor
5. https://www.onetrust.com/blog/third-party-risk-management/
6. https://www.corporatecomplianceinsights.com/wp-content/uploads/2017/11/Framework-for-a-Third-Party-Risk-Management-Program-2016-09-22-13.58.pdf

7. https://economictimes.indiatimes.com/news/company/corporate-trends/india-inc-has-highest-cost-reduction-targets-deloitte-survey/articleshow/60086548.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

8. https://www.businesstoday.in/latest/trends/story/india-ranks-third-in-global-data-breaches-in-2021-report-315750-2021-12-15